

Cảnh báo 12 lỗ hổng có mức độ ảnh hưởng cao và nghiêm trọng ở sản phẩm của Microsoft

22:17 18/02/2023

Cục An toàn thông tin, Bộ Thông tin và Truyền thông đã lưu ý các đơn vị chuyên trách công nghệ thông tin, an toàn thông tin; các tập đoàn, tổng công ty nhà nước cùng các ngân hàng, tổ chức tài chính về 12 lỗ hổng có mức độ ảnh hưởng cao và nghiêm trọng.



Ảnh minh họa. (Ảnh: internet)

Có mức ảnh hưởng nghiêm trọng với điểm CVSS 9.8, lỗ hổng bảo mật CVE-2023-21716 trong Microsoft Word cho phép đối tượng tấn công thực thi mã từ xa.

Lỗ hổng CVE-2023-21715 tồn tại trong Microsoft Publisher có mức ảnh hưởng cao, cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật. Lỗ hổng này đang bị khai thác trên thực tế.

Cùng có ảnh hưởng mức cao, 2 lỗ hổng CVE-2023-23376 và CVE-2023-21812 trong Windows Common Log File System (CLFS) cho phép đối tượng tấn công

thực hiện tấn công nâng cao đặc quyền. Cả 2 lỗ hổng này, theo Cục An toàn thông tin, đều đang bị khai thác.

Ba lỗ hổng CVE-2023-21705, CVE-2023-21713, CVE-2023-21528 trong Microsoft SQL Server cho phép đối tượng tấn công thực thi mã từ xa.

Lỗ hổng bảo mật CVE-2023-21717 trong Microsoft SharePoint Server cho phép đối tượng tấn công thực hiện nâng cao đặc quyền.

Các chuyên gia Cục An toàn thông tin đặc biệt lưu ý 4 lỗ hổng CVE-2023-21529, CVE-2023-21710, CVE-2023-21707 và CVE-2023-21706 trong Microsoft Exchange Server. Các lỗ hổng bảo mật cho phép đối tượng tấn công thực thi mã từ xa.

Theo đánh giá của Cục An toàn thông tin, Microsoft Exchange Server đã và đang là mục tiêu hàng đầu được các nhóm tấn công có chủ đích - APT. Vì vậy, các cơ quan, tổ chức cần đặc biệt chú ý cũng như có kế hoạch khắc phục và tăng cường giám sát nhằm giảm thiểu và tránh nguy cơ bị tấn công thông qua các lỗ hổng này.

Hà Trần (t/h)